2.2

2.2.1

For any natural numbers a, b, c, we have $(a + b) + c = a + (b + c)$.

Proof. Induct on b by keeping a and c fixed. Consider the base case $b = 0$. In this case, LHS$= (a + 0) + c = a + c$ and RHS$= a + (0 + c) = a + c$. Now suppose that $(a+b)+c = a+(b+c)$. We need to show that $(a+(b++))+c = a+((b++)+c)$:

$$\begin{aligned}\text{LHS} &= (a + (b + +)) + c = ((a + b) + +) + c = (a + b + c) + +, \\ \text{RHS} &= a + ((b + +) + c) = a + ((b + c) + +) = (a + b + c) + +.\end{aligned}$$

Thus both sides are equal to each other, and we have closed the induction. □

2.2.2

Let a be a positive number. Then there exists exactly one natural number b such that $b + + = a$. (I'm assuming that it meant a is a positive natural number.)

Proof. Induct on a. Since 0 is not positive, we consider the base case $a = 1$. We have $b++ = b+1 = 0+1 = 1$. Cancellation law tells us that $b = 0$, which is unique. Now suppose that there exists exactly one natural number b_0 such that $b_0 + + = a$, we need to show that there exists exactly one natural number b such that $b++ = a++$. By Cancellation law, we have $b = a = b_0 + +$. Since b is the successor of b_0 and b_0 is unique, b is also unique. Thus we have closed the induction. □

2.2.3

(a)

$a \geq a$.

Proof. There exists a natural number 0 such that $a + 0 = a$. Thus, $a \geq a$. □

(b)

If $a \geq b$ and $b \geq c$, then $a \geq c$.

Proof. Since $a \geq b$, there exists a natural number m such that $b + m = a$. Since $b \geq c$, there exists a natural number n such that $c + n = b$. Then $c + (n + m) = (c + n) + m = b + m = a$. Therefore, $c \geq a$.

Thus, if $a \geq b$ and $b \geq c$, then $a \geq c$. □

(c)

If $a \geq b$ and $b \geq a$, then $a = b$.

Proof. Since $a \geq b$, there exists a natural number m such that $b + m = a$. Since $b \geq a$, there exists a natural number n such that $a + n = b$. Then we have $a + n = (b + m) + n = b + (m + n) = b$. By Cancellation law, we have $m + n = 0$ which leads to $m = 0$, $n = 0$. Thus, $a = a + 0 = b$.

Thus, if $a \geq b$ and $b \geq a$, then $a = b$. □

(d)

$a \geq b$ if and only if $a + c \geq b + c$.

Proof. First, we need to show that $a \geq b \Rightarrow a + c \geq b + c$. Since $a \geq b$, there exists a natural number n such that $b + n = a$. Then we have $b + n + c = b + c + n = (b + c) + n = a + c$. Thus, $a + c \geq b + c$. Then, we need to show that $a + c \geq b + c \Rightarrow a \geq b$. Since $a + c \geq b + c$, there should be a natural number n such that $b + c + n = b + n + c = (b + n) + c = a + c$. By Cancellation law, we have $b + n = a$. Thus, $a \geq b$.

Thus, if $a \geq b$ and $b \geq a$, then $a = b$. □

(e)

$a < b$ if and only if $a{+}{+} \leq b$.

Proof. First, we need to show that $a < b \Rightarrow a++ \leq b$. $a < b$ means there exists a natural number n such that $a + n = b$, particularly, $a \neq b$. Then n must not be zero. So n is the predecessor of a natural number, denote it as m. Then we have $a + n = a + (m++) = (a + m)++ = (a++) + m = b$. Therefore, $a++ \leq b$. Then we need to show that $a++ \leq b \Rightarrow a < b$. There exists a natural number n such that $(a++) + n = b$. $(a++) + n = (a + n)++ = a + (n++) = b$. Since $n++$ is the successor of n, $n++$ must not be equal to 0. If $a = b$, there will be $a + (n++) = a \Rightarrow n++ = 0$, contradiction. Therefore, $a \neq b$.

Thus, $a < b$ if and only if $a++ \leq b$. □

(f)

$a < b$ if and only if $b = a + d$ for some positive number d.

Proof. First, we need to show that $a < b \Rightarrow b = a + d$ for some positive number d. There exists some natural number d such that $a + d = b$, $a \neq b$. By Cancellation law, d must not be zero. Therefore, d is positive. Then, we need to show that $a + d = b$ for some positive $d \Rightarrow a < b$. We only need to prove $a \neq b$. If $a = b$, we have $a + d = a = a + 0$. By Cancellation law, $d = 0$ which contradicts to d is positive. Therefore, $a \neq b$.

Thus, $a < b$ if and only if $b = a + d$ for some positive number d. □

2.2.4

Justify the three statements marked in the proof of Proposition 2.2.13.

(a)

$0 \leq b$ for all b.

Proof. By definition of addition, we have $0 + b = b$. Thus, $0 \leq b$. □

(b)

If $a > b$, then $a++ > b$.

Proof. By Proposition 2.2.12.e, we have $a > b \Rightarrow a \geq b++$. And by Proposition 2.2.12.d, $a + 1 \geq (b++) + 1$ that is equivalent to $a++ \geq b + 2$. Since 2 is positive, by Proposition 2.2.12.f, we have $a++ > b$. □

(c)

If $a = b$, then $a++ > b$.

Proof. We know from Proposition 2.2.12.a that $a \geq a$, so $a \geq a = b$. And again by Proposition 2.2.12.d, we have $a{++} = a{+}1 \geq b{+}1$. Since 1 is positive, by Proposition 2.2.12.f, $a++ > b$.

□

2.2.5

Proposition 2.2.14 (Strong principle of induction). Let m_0 be a natural number, and let $P(m)$ be a property pertaining to an arbitrary natural number m. Suppose that for each $m \geq m_0$, we have the following implication: if $P(m')$ is true for all natural numbers $m_0 \leq m' < m$, then $P(m)$ is also true. Then we can conclude that $P(m)$ is true for all natural numbers $m \geq m_0$.

Proof. Let $Q(n)$ be the property that $P(m)$ is true for all $m_0 \leq m < n$. Induct on n. Consider the base case $n = 0$. This is vacuously true. In fact, $Q(n)$ is vacuously true for all $n \leq m_0$. So we can assume $n > m_0$ to see if the implication stands. Suppose $Q(n)$ is true, that is, $P(m)$ is true for all $m_0 \leq m < n$. We want to show that $Q(n{+}1)$ is also true. As stated in Proposition 2.2.14, if $Q(n)$ is true, then $P(n)$ is also true. So $P(m)$ is true for all $m_0 \leq m \leq n$. Hence, $P(m)$ is true for all $m_0 \leq m < n + 1$. ($m \leq n \Leftrightarrow m < n + 1$ can be shown using prop 2.2.12.) Thus, $Q(n + 1)$ is true. This closes the induction. □

2.2.6

Let n be a natural number, and let $P(m)$ be a property pertaining to the natural numbers such that whenever $P(m{++})$ is true, then $P(m)$ is true. Suppose that $P(n)$

is also true. Prove that $P(m)$ is true for all natural numbers $m \leq n$. (Principle of backwards induction.)

Proof. Apply induction to n. For the base case $n = 0$, suppose $P(0)$ is true. In this case, m can only be 0 ($m + k = 0 \Rightarrow m = 0, k = 0$). Since $P(0)$ is true, the base case is proved. Next, suppose if $P(n)$ is true then $P(m)$ is true for all natural numbers $m \leq n$. We want to show that if $P(n++)$ is true then $P(m)$ is true for all natural numbers $m \leq n++$. $m \leq n$ means there exists a natural number a such that $m + a = n++$. a is either 0 or a positive number. If a is 0, $m = n++$. If a is positive, $m < n++$ (by prop 2.2.12.f), this is equivalent to $m \leq n$ (can be shown using prop 2.2.12.). For $m = n++$, $P(m)$ is true because of the assumption. For each $m \leq n$, $P(m)$ is also true by induction hypothesis. Therefore, $P(m)$ is true for all natural numbers $m \leq n++$. And we have closed the induction. $\square$

In the above proofs, $n++$ and $n+1$ got mixed up because $n++ = n+1$ has been illustrated on Page 26 (and the +1 version is a little easier). But ++ is a more desirable expression since it stands for the successor in a general way.

2.3

Definition 2.3.1 (Multiplication of natural numbers).

Let m be a natural number. To multiply zero to m, we define $0 \times m := 0$. Now suppose inductively that we have defined how to multiply n to m. Then we can multiply $n++$ to m by defining $(n++) \times m := (n \times m) + m$.

2.3.1

Lemma 2.3.2 (Multiplication is commutatitive). Let n, m be natural numbers. Then $n \times m = m \times n$.

Proof. First, we want to show that $m \times 0 = 0$. Induct on m. When $m = 0$, by definition $0 \times m = 0$ for every m, so $0 \times 0 = 0$. Suppose $m \times 0 = 0$, we want to show that $(m++) \times 0 = 0$. By definition, we got $(m++) \times 0 = (m \times 0) + 0$ which is equal to $0 + 0 = 0$. This closes the induction.

Then, we want to show that $n \times (m++) = n \times m + n$. Induct on n by keeping m fixed. Consider the base case $n = 0$. The LHS is equal to $0 \times (m++) = 0$ by definition. The RHS is equal to $0 \times m + 0$ which is also 0. Now suppose inductively $n \times (m++) = n \times m + n$. We need to show that $(n++) \times (m++) = (n++) \times m + (n++)$.

$$\begin{aligned}
\text{LHS} &= (n++) \times (m++) = n \times (m++) + (m++) \\
&= n \times m + n + (m++) = n \times m + (n + m)++, \\
\text{RHS} &= (n++) \times m + (n++) = n \times m + m + (n++) = n \times m + (n + m)++.
\end{aligned}$$

Thus, both sides are equal to each other. This closes the induction.

Now we can use the things above to show Lemma 2.3.2. We induct on n by keeping m fixed. Consider the base case $n = 0$. $0 \times m = m \times 0 = 0$ by definition and the lemma we have shown above. Assume inductively $n \times m = m \times n$. We want to show that $(n++) \times m = m \times (n++)$. By definition, the LHS is equal to $(n++) \times m = (n \times m) + m$. By the lemma we proved above, the RHS is equal to $m \times (n++) = m \times n + m = n \times m + m$. So both sides are equal to each other. We have closed the induction. $\square$

2.3.2

Lemma 2.3.3 (Positive natural numbers have no zero divisors). Let n, m be natural numbers. Then $n \times m = 0$ if and only if at least one of m, n is equal to zero. In particular, if n and m are both positive, then nm is also positive.

Proof. Try to prove the second statement first. Assume n, m are both positive natural numbers. So we can represent n as $a++$ where a is a natural number. Then

$$\begin{aligned}
nm &= (a++) \times m \\
&= a \times m + m.
\end{aligned}$$

Since m is positive and $a \times m$ is at least 0, $nm = a \times m + m$ must be positive. In this sense, we have shown $n \times m = 0 \Rightarrow$ at least one of n, m is zero since

$p \to q \equiv \; q \to \; p$. The rest part is to show at least one of n, m is zero $\Rightarrow n \times m = 0$. This is trivial and can be directly proved using the definition.

Thus, $n \times m = 0$ if and only if at least one of m, n is equal to zero. $\square$

2.3.3

Proposition 2.3.5 (Multiplication is associative). For any natural numbers a, b, c, we have $(a \times b) \times c = a \times (b \times c)$.

Proof. Fix a, c and induct on b. Consider the base case when $b = 0$.

$$\begin{aligned} \text{LHS} &= (a \times 0) \times c = 0 \times c = 0, \\ \text{RHS} &= a \times (0 \times c) = a \times 0 = 0. \end{aligned}$$

Thus, the base case is proved. Assume inductively $(a \times b) \times c = a \times (b \times c)$. We need to show that $(a \times (b++)) \times c = a \times ((b++) \times c)$.

$$\begin{aligned} \text{LHS} &= (a \times (b++)) \times c = (a \times b + a) \times c = (a \times b) \times c + ac, \\ \text{RHS} &= a \times ((b++) \times c) = a \times (b \times c + c) = a \times (b \times c) + ac. \end{aligned}$$

By induction hypothesis, $(a \times b) \times c = a \times (b \times c)$. Thus, both sides are equal to each other. This closes the induction. $\square$

2.3.4

Prove the identity $(a + b)^2 = a^2 + 2ab + b^2$ for all natural numbers a, b.

Proof. Suppose a is an arbitrary natural number and keep a fixed. Induct on b. First consider the base case $b = 0$.

$$\begin{aligned} \text{LHS} &= (a + 0)^2 = a^2, \\ \text{RHS} &= a^2 + 2ab + b^2 = a^2 + 0 + 0 = a^2. \end{aligned}$$

So the base case is proved. Now assume inductively $(a+b)^2 = a^2+2ab+b^2$. We need to show that $(a + (b++))^2 = a^2 + 2a(b++) + (b++)^2$.

$$\begin{aligned}
\text{LHS} &= (a + (b++))^2 \\
&= ((a + b)++)^2 \\
&= ((a + b)++) \times ((a + b)++) \\
&= (a + b)(a + b) + (a + b) + (a + b)++ \\
&= \underbrace{a^2 + 2ab + b^2}_{\text{by induction hypothesis}} + (2a + 2b)++, \\
\text{RHS} &= a^2 + 2a(b++) + (b++)^2 \\
&= a^2 + 2ab + 2a + b(b++) + (b++) \\
&= a^2 + 2ab + 2a + b^2 + b + (b++) \\
&= a^2 + 2ab + b^2 + (2a + 2b)++.
\end{aligned}$$

Thus, both sides are equal to each other. This closes the induction. □

2.3.5

Proposition 2.3.9 (Euclidean algorithm). Let n be a natural number, and let q be a positive number. Then there exist natural numbers m, r such that $0 \le r < q$ and $n = mq + r$.

Proof. Fix q and induct on n. Consider the base case $n = 0$. Let $m = 0, r = 0$, then $mq + r = 0 \times q + 0 = 0$ as required. Now assume inductively there exist natural numbers m, r such that $0 \le r < q$ and $n = mq + r$. What we want to show is there exist natural numbers m', r' such that $0 \le r' < q$ and $n + 1 = m'q + r'$. Since $r < q$, we have two cases: $r + 1 < q$ and $r + 1 = q$.
Case 1: $r+1 < q$. Let $m' = m$, $r' = r+1$, $0 \le r' < q$. Then $m'q+r' = mq+(r+1) = (mq + r) + 1 = n + 1$ as required.
Case 2: $r + 1 = q$. $n + 1 = mq + (r + 1)$ since $n = mq + r$ by induction hypothesis. Substitute $(r+1)$ with q, we have $n+1 = mq+q = (m+1)q$. Let $m' = m+1, r' = 0$. We got $n + 1 = m'q + r'$ as required. We got $n + 1 = m'q + r'$ as required. Thus, we have closed the induction. □